



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/991,842	11/19/2001	Charles Douglas Blewett	2001-0057	6013

26652 7590 04/06/2005

AT&T CORP.  
P.O. BOX 4110  
MIDDLETOWN, NJ 07748

EXAMINER

LEMMA, SAMSON B

ART UNIT	PAPER NUMBER
----------	--------------

2132

DATE MAILED: 04/06/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

## Office Action Summary

Application No.

09/991,842

Applicant(s)

BLEWETT ET AL.

Examiner

Samson B Lemma

Art Unit

2132

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --  
Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

### Status

- 1) ☒ Responsive to communication(s) filed on 19 November 2001.
- 2a) ☐ This action is **FINAL**. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

### Disposition of Claims

- 4) ☒ Claim(s) 1-58 is/are pending in the application.
- 4a) Of the above claim(s) \_\_\_\_\_ is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-58 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

### Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).  
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

### Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some \* c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
  - ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.
  - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).
- \* See the attached detailed Office action for a list of the certified copies not received.

### Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)  
Paper No(s)/Mail Date 4.
- 4) ☐ Interview Summary (PTO-413)  
Paper No(s)/Mail Date. \_\_\_\_\_.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: \_\_\_\_\_.

## ***DETAILED ACTION***

1. **Claims 1-58** have been examined.

### ***Double Patenting***

2. The nonstatutory double patenting rejection is based on a judicially created doctrine grounded in public policy (a policy reflected in the statute) so as to prevent the unjustified or improper timewise extension of the "right to exclude" granted by a patent and to prevent possible harassment by multiple assignees. See *In re Goodman*, 11 F.3d 1046, 29 USPQ2d 2010 (Fed. Cir. 1993); *In re Longi*, 759 F.2d 887, 225 USPQ 645 (Fed. Cir. 1985); *In re Van Ornum*, 686 F.2d 937, 214 USPQ 761 (CCPA 1982); *In re Vogel*, 422 F.2d 438, 164 USPQ 619 (CCPA 1970); and, *In re Thorington*, 418 F.2d 528, 163 USPQ 644 (CCPA 1969).

A timely filed terminal disclaimer in compliance with 37 CFR 1.321(c) may be used to overcome an actual or provisional rejection based on a nonstatutory double patenting ground provided the conflicting application or patent is shown to be commonly owned with this application. See 37 CFR 1.130(b).

Effective January 1, 1994, a registered attorney or agent of record may sign a terminal disclaimer. A terminal disclaimer signed by the assignee must fully comply with 37 CFR 3.73(b).

3. **Claims 1-58** are provisionally rejected under the judicially created doctrine of obviousness-type double patenting as being unpatentable over **claims 1-60** of the copending Application No. 09/991844 (hereinafter referred as '**844 application**). Although the conflicting claims are not identical, they are not patentably distinct from each other.

This is a provisional obviousness-type double patenting rejection because the conflicting claims have not in fact been patented.

#### **The following is referring to the independent claims**

- **As per claim 1**, claim 1 of the instant application and claim 1 of the '**844 application** recite similar/same limitation about the security gateway for

Art Unit: 2132

securely connecting a plurality of networks. Furthermore, all elements/limitation of **claim 1** of the instant application is recited in the **claim 1** of the '844 application, except **claim 1** of '844 application at the end of the claim contains the following extra limitation which is not included in the instant claim **"Permitting at least some limited clients access through the gateway from the host in the untrusted network to a host in the second network "**. Otherwise, all elements/limitation of claim 1 of the instant application is recited in the claim 1 of the '844 application. Therefore, for the reason given above, **claim 1** which is rejected for double patenting **is anticipated** by **claim 1** of the '844 application.

- **As per claim 25, claim 25** of the instant application and **claim 21** of the '844 application recite similar/same limitation about security gateway for securely connecting a plurality of networks. Furthermore, all elements/limitation of **claim 25** of the instant application is recited in the **claim 21** of the '844 application, except **claim 21** of '844 application at the end of the claim contains the following extra limitation which is not included in the instant claim **"Permitting at least some limited clients access through the gateway from the host in the untrusted network to a host in the second network "**. Otherwise, all elements/limitation of **claim 25** of the instant application is recited in the **claim 21** of the '844 application. Therefore, for the reason given above, **claim 25** which is rejected for double patenting **is anticipated** by **claim 21** of the '844 application.

- **As per claim 42, claim 42** of the instant application and **claim 41** of the '844 application recite similar/same limitation about security gateway for securely connecting a plurality of networks and all elements/limitation of **claim**

Art Unit: 2132

**42** of the instant application is recited in the **claim 41** of the **'844** application, except **claim 41** of **'844** application at the end of the claim contains the following extra limitation which is not included in the instant claim **"Permitting at least some limited clients access through the gateway from the host in the untrusted network to a host in the second network "**. Otherwise, all elements/limitation of **claim 42** of the instant application is recited in the **claim 41** of the **'844** application. Therefore, for the reason given above, **claim 42** which is rejected for double patenting **is anticipated by claim 41** of the **'844** application.

**The following is referring to the dependent claims**

- **As per claims 2, 26 and 43** **claims 2, 26 and 43** of the instant application and **claims 5 ,25 and 45** of the **'844** application further recite similar/same limitation.
- **As per claims 3, 27 and 44** **claims 3, 27 and 44** of the instant application and **claims 6 ,26 and 46** of the **'844** application further recite similar/same limitation.
- **As per claims 4, 24, 28 and 45** **claim 4, 24, 28 and 45** of the instant application and **claims 7, 27 and 47** of the **'844** application further recite similar/same limitation.
- **As per claims 5, 29 and 46** **claim 5, 29 and 46** of the instant application and **claims 8, 28 and 48** of the **'844** application further recite similar/same limitation.
- **As per claims 6, 30 and 47** **claim 6, 30 and 47** of the instant application and **claims 9, 29 and 49** of the **'844** application further recite similar/same limitation.

Art Unit: 2132

- **As per claims 7, 31 and 48** claim 7, 31 and 48 of the instant application and **claims 10, 30 and 50** of the '844 application further recite similar/same limitation.
- **As per claims 8, 32 and 49** claim 8, 32 and 49 of the instant application and **claims 11, 31 and 51** of the '844 application further recite similar/same limitation.
- **As per claims 9, 23, 33 and 50** claim 9, 23,33 and 50 of the instant application and **claims 12, 32 and 52** of the '844 application further recite similar/same limitation.
- **As per claims 10, 34 and 51** claim 10, 34 and 51 of the instant application and **claims 13, 33 and 53** of the '844 application further recite similar/same limitation.
- **As per claims 11, 35 and 52** claim 11, 35 and 52 of the instant application and **claims 14, 34 and 54** of the '844 application further recite similar/same limitation.
- **As per claims 12, 36 and 53** claim 12, 36 and 53 of the instant application and **claims 15, 35 and 55** of the '844 application further recite similar/same limitation.
- **As per claims 13, 37 and 54** claim 13, 37 and 54 of the instant application and **claims 16, 36 and 56** of the '844 application further recite similar/same limitation.
- **As per claims 14, 22, 38, and 55** claim 14, 22,38 and 55 of the instant application and **claims 17, 37 and 57** of the '844 application further recite similar/same limitation.
- **As per claims 15, 39 and 56** claim 15, 39 and 56 of the instant application and **claims 18, 38 and 58** of the '844 application further recite similar/same limitation.

Art Unit: 2132

- **As per claims 16, 40 and 57 claim 16, 40 and 57** of the instant application and **claims 19, 39 and 59** of the '844 application further recite similar/same limitation.
- **As per claims 17, 41 and 58 claim 17, 41 and 58** of the instant application and **claims 20, 40 and 60** of the '844 application further recite similar/same limitation.
- **As per claims 18, 19 and 20 claim 18, 19 and 20** of the instant application and **claims 1, 21 and 41** of the '844 application further recite similar/same limitation.

### ***Claim Objections***

4. **Claims 3, 6 and 11** are objected to because of the following informalities:
- Claims **3, 6 and 11** recite the following "...wherein the packet handling rules for **translating translate** the source network address ..." The word "**translate**" has to be removed.
- Appropriate correction is required.

### ***Claim Rejections - 35 USC § 102***

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

A person shall be entitled to a patent unless –

(e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

Art Unit: 2132

6. ~~**Claims 1-2, 4, 7-9, 12-26, 28, 31-33, 36-43, 45, 48-50, 55-58**~~ are rejected under 35 U.S.C. 102(e) as being anticipated by **Flint et al.** (hereinafter referred to as **Flint**) (U.S. Patent No. 6,453,419).

7. ~~**As per claims 1, 4, 7-9, 12, 15-17, 19, 21, 23-25, 28, 31-33, 36, 39-42, 45, 48-50, 56-58**~~ **Flint** discloses a security gateway [firewall, shown on figure 2, ref. Num "34" and discussed on column 1, lines 21-32] **for securely connecting a plurality of networks;**[column 2, lines 13; figure 2, ref. Num "32", "46", "36" and "42"; column 3, lines 32-46] (The security gateway or the **firewall shown on figure 2, ref. Num "34"** connects a plurality of networks as shown on figure 2, ref. Num "32", "46", "36" and "42" and these networks shown on figure 2, is formed by **grouping together networks** that requires the same type of security as explained on column 3, lines 21-23) **comprising:**

- **A logical interface to a first network;** [Figure 2, ref. Num "32" and ref. Num "34"] (The first network or the internal network or the company private network shown on figure 2, ref. Num "32" is interfaced to the firewall/security gateway shown on figure 2, ref. Num "34". In other words, there is a logical interface from the firewall/security gateway to the first network/internal network or company private network)

- **A logical interface to a second network;** [Figure 2, ref. Num "42" and ref. Num "34"] (The second network or the secure server network shown on figure 2, ref. Num "42" is interfaced to the firewall or the security gateway shown on figure 2, ref. Num "34". In other words, there is a logical interface from the the firewall/security gateway to the second network)



Art Unit: 2132

- **A physical interface to a third network that is an untrusted network;** [Figure 2, ref. Num “36” and ref. Num “34”] (The untrusted network or the internet shown on figure 2, ref. Num “36” is interfaced to the firewall/security gateway shown on figure 2, ref. Num “34”. In other words, there is a physical interface from the firewall/security gateway to the untrusted network/the internet.)
- **A logical interface to a fourth network that is a protected resource work;** [Figure 2, ref. Num “46” and ref. Num “34”] (The fourth network or the Partner Shared Network shown on figure 2, ref. Num “46” is interfaced to the firewall/security gateway shown on figure 2, ref. Num “34”. In other words, there is a logical interface from the firewall/security gateway to the fourth network/Partner Shared networks)
- **A processor** [inherently included in the Kernel; since a kernel manages the machine’s hardware resources including the “processor” and the “memory”] **configured to execute packet handling rules for** [column 4, lines 14-17; column 21, lines 42-44] (All the codes that implements the access rules are included in the kernel as explained on column 4, lines 15-16. The access control list the rules are in the kernel and the ACLs are the heart and brains of the access policy/rules of the firewall/security gateway as explained on column 21 lines 42-46) ;
- **Denying at least some client access through the gateway from a host in the untrusted network to hosts in the first network, in the second network and in the protected resource network;** [Column 3, lines 48-60; column 3, line 61-column 4, line 6; figure 4, ref. Num “66”] (Every access coming from the source/could be from any of the four networks connected to the firewall shown as shown on figure 2, to the destination which could also be

Art Unit: 2132

any of the four networks that are connected to the firewall as shown on figure 2, ref. Num "34" passes through the security gateway/firewall shown on figure 2, ref. Num "34". The access request will be **allowed/permitted or denied** based on the comparison of the request to the access control rules as explained on column 2, lines 38-42 and/or based on the user or groups initiating the connection request or the IP address of the host of the connection as explained on column 4, lines 1-2. The incoming request **is allowed or denied** based on the results of the node/access rules comparison as explained on column 4, lines 4-7 and the source and the destination of the networks/regions as explained on column 29-31 or based on any users building decision tree created by the user consisting of the desired options as explained on column 6, lines 6-11. Therefore denying or permitting some client access through the gateway is inherently included as explained above.)

- **Denying at least some client access through the gateway from a host in the second network to a host in the first network** [Column 3, lines 48-60; column 3, line 61-column 4, line 6; figure 4, ref. Num "66"] (Every access coming from the source/could be from any of the four networks connected to the firewall shown as shown on figure 2, to the destination which could also be any of the four networks that are connected to the firewall as shown on figure 2, ref. Num "34" passes through the security gateway/firewall shown on figure 2, ref. Num "34". The access request will be **allowed/permitted or denied** based on the comparison of the request to the access control rules as explained on column 2, lines 38-42 and/or based on the user or groups initiating the connection request or the IP address of the host of the connection as explained on column 4, lines 1-2. The incoming request **is allowed or denied** based on the results of the node/access rules comparison as explained on column 4, lines 4-7 and the source and the destination of the networks/regions

Art Unit: 2132

as explained on column 29-31 or based on any users building decision tree created by the user consisting of the desired options as explained on column 6, lines 6-11. Therefore denying or permitting some client access through the gateway is inherently included as explained above.)

**and**

• **Permitting at least some client access through the gateway from a host in the first network to hosts in the second network and in the protected resource network.**[Figure 4, ref. Num "64"; column 3, lines 48-60; column 3, line 61-column 4, line 6; figure 4, ref. Num "66"] (Every access coming from the source/could be from any of the four networks connected to the firewall shown as shown on figure 2, to the destination which could also be any of the four networks that are connected to the firewall as shown on figure 2, ref. Num "34" passes through the security gateway/firewall shown on figure 2, ref. Num "34". The access request will be **allowed/permited or denied** based on the comparison of the request to the access control rules as explained on column 2, lines 38-42 and/or based on the user or groups initiating the connection request or the IP address of the host of the connection as explained on column 4, lines 1-2. The incoming request **is allowed or denied** based on the results of the node/access rules comparison as explained on column 4, lines 4-7 and the source and the destination of the networks/regions as explained on column 29-31 or based on any users building decision tree created by the user consisting of the desired options as explained on column 6, lines 6-11. Therefore denying or permitting some client access through the gateway is inherently included as explained above.)

8. **As per claims 2, 26 and 43 Flint** discloses the security gateway as applied to claims 1, 25 and 42 above. Furthermore **Flint** discloses the security gateway, wherein

Art Unit: 2132

the processor is further configured to execute packet handling rules for **translating a source network address in a packet sent to the second network**. [Column 5, lines 5-12] (A rewrite node is a point in an access rule where source or destination address are mapped to the other source or destination address as explained on column 5, lines 5-12)

9. **As per claims 13 and 37** Flint discloses the security gateway as applied to claims above. Furthermore **Flint** discloses the security gateway, wherein the protected network service is a mail relay.[Column 12, lines 11-14] (As explained on column 12, lines 11-14, there are a number of email filters required. This includes mail mapping and content blocking. Again the proxy/server must fulfill the requirements of the filter and the protected network could contain such a server and meets the recitation of these claims.)

10. **As per claims 14, 22 and 38 and 55** Flint discloses the security gateway as applied to claims 1, 21, 25 and 42 above. Furthermore **Flint** discloses the security gateway, wherein the interface to the protected resource network includes a VPN tunnel utilizing the un trusted network.[Figure 2, ref. Num "45"]

11. **As per claims 18** Flint discloses the security gateway as applied to claims 1, above. Furthermore **Flint** discloses the security gateway, wherein the logical interface to the first network is a logical interface to a first trust-group network, and the logical interface to the-second network is a logical interface to a second trust-group network.[column 3, lines 21-23] (The network are formed by grouping together networks that require the same type of security as explained

Art Unit: 2132

on column 3, lines 21-23 and shown on figure 2, ref. Num "46" and "36" and "42" and "32" meets the recitation of this claims.)

12. **As per claims 20** **Flint** discloses the security gateway as applied to claims 1, above. Furthermore **Flint** discloses the security gateway, wherein the logical interface to the protected resource network is a logical interface to a remote corporate network. [figure 2, ref. Num "46"] (The Partner shared network/protected resource network which is logically interfaced to the gateway as shown on figure 2, ref. Num "45" meets the recitation of this claim.)

### ***Claim Rejections - 35 USC § 103***

13. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

14. **Claims 3, 5-6, 10-11, 27, 29-30, 34-35, 44, 46-47, 51-54** are rejected under 35 U.S.C. 103(a) as being unpatentable over **Flint et al.** (hereinafter referred to as **Flint**) (U.S. Patent No. 6,453,419) in view of **Chopra et al.** (hereinafter referred to as **Chopra**) (U.S. Patent No. 6,611,875 B1)

15. **As per claims 5-6, 10-11, 29-30, 34-35, 46-47, 51-52** **Flint** discloses the security gateway/firewall as applied to claims above. Furthermore **Flint** discloses the method, wherein the processor is further configured to execute packet handling

Art Unit: 2132

rules for **translating a source network address in a packet sent to the second network**. [Column 5, lines 5-12] (A rewrite node is a point in an access rule where source or destination address are mapped to the other source or destination address as explained on column 5, lines 5-12).

**Flint** does not explicitly disclose the security gateway, wherein the packet handling rules for translating the source network address of a packet sent to the un trusted network to be the network address of the security gateway interface to the un trusted network.

However, in the same field of endeavor, **Chopra** discloses a control system for high-speed rule processors used in a gateway system is disclosed. The gateway system employing the current invention can process packets at wire speed by using massive parallel processors, each of the processors operating concurrently and independently.[Abstract, lines 1-5]. Furthermore **Chopra** discloses the gateway wherein when an internal workstation: 142, 144, 146, or 148 wishes to initiate communication with a server (121 or 123) on the Internet/untrusted network, the Internet gateway 130 **intercepts the communication and replaces the internal workstation's source address with a fully-qualified Internet address held by the Internet gateway 130**. [column 4, lines 65-column 5, line 3]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of Network address translation for translating the source address which is destined to the un trusted network or the internet as per teachings of **Chopra in to the method of** as taught by **Flint** in order to **conceal** the actual network addresses of the source within the protected networks, discouraging attacks from the un trusted network.

Art Unit: 2132

16. **As per claims 3, 27 and 44 Flint** discloses the security gateway/firewall as applied to claims above. Furthermore **Flint** discloses the method, wherein the processor is further configured to execute packet handling rules for **translating a source network address in a packet sent to the destination network**.

[Column 5, lines 5-12] (A rewrite node is a point in an access rule where source or destination address are mapped to the other source or destination address as explained on column 5, lines 5-12).

**Flint** does not explicitly disclose the security gateway, wherein the packet handling rules for translating a source network address in a packet sent to the second network to be the network address of the security gateway interface to the second network.

However, in the same field of endeavor, **Chopra** discloses a control system for high-speed rule processors used in a gateway system is disclosed. The gateway system employing the current invention can process packets at wire speed by using massive parallel processors, each of the processors operating concurrently and independently. [Abstract, lines 1-5]. Furthermore **Chopra** discloses when the Internet server responds and when the respond is destined to the internal network which could be the second network or any network in the LAN, **the Internet gateway 130 will translate the fully-qualified internet address back into the workstation's internal address and pass the packet onto the internal LAN 140**. [Column 4, lines 65-Column 5, line 6]

It would have been obvious to one having ordinary skill in the art, at the time the invention was made, to combine the features of Network address translation for translating the source address which is destined to any protected network or the 2<sup>nd</sup> network in this case as per teachings of **Chopra in to the method** as taught by **Flint** in order to **conceal** the actual network addresses of the source to conceal and secure the source.

17. **As per claims 53,** the combination of **Flint and Chopra** discloses the security gateway as applied to claims 52 above. Furthermore, **Flint** discloses the security gateway further has a protected network service, and the method further comprises the step of denying at least some access from at least one network to the protected network service. [Column 3, lines 48-60; column 3, line 61-column 4, line 6; figure 4, ref. Num "66"] (Every access coming from the source/could be from any of the four networks connected to the firewall shown as shown on figure 2, to the destination which could also be any of the four networks that are connected to the firewall as shown on figure 2, ref. Num "34" passes through the security gateway/firewall shown on figure 2, ref. Num "34". The access request will be **allowed/permitted or denied** based on the comparison of the request to the access control rules as explained on column 2, lines 38-42 and/or based on the user or groups initiating the connection request or the IP address of the host of the connection as explained on column 4, lines 1-2. The incoming request **is allowed or denied** based on the results of the node/access rules comparison as explained on column 4, lines 4-7 and the source and the destination of the networks/regions as explained on column 29-31 or based on any users building decision tree created by the user consisting of the desired options as explained on column 6, lines 6-11. Therefore denying or permitting some client access through the gateway is inherently included as explained above.)
18. **As per claims 54,** the combination of **Flint and Chopra** discloses the security gateway as applied to claims 53 above. Furthermore, **Flint** discloses the security gateway wherein the protected network service is a mail relay.[Column 12, lines 11-14] (As explained on column 12, lines 11-14, there are a number of email filters required.



Art Unit: 2132

This includes mail mapping and content blocking. Again the proxy/server must fulfill the requirements of the filter and the protected network could contain such a server and meets the recitation of these claims.)

### ***Conclusion***

19. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure. (See PTO-Form 892).

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Samson B Lemma whose telephone number is 571-272-3806. The examiner can normally be reached on Monday-Friday (8:00 am---4: 30 pm).

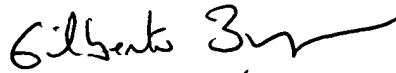
If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, BARRON JR GILBERTO can be reached on. The fax phone number for the organization where this application or proceeding is assigned is 571-272-3799.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

SAMSON LEMMA

**S.L.**

03/28/2005

  
GILBERTO BARRÓN JR.  
SUPERVISORY PATENT EXAMINER  
TECHNOLOGY CENTER 2100